LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS FRENTE A LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Rojas Villamil, Carlos Michael
carrovi8847@gmail.com
Universidad Piloto de Colombia

Resumen— El Ministerio de las Tecnologías de la Información y las Comunicaciones MinTIC estableció un manual con el cual se imparte responsabilidades ente caso a la Universidad Distrital Francisco José de Caldas para implementar entre varias actividades un Sistema de Gestión de Seguridad de la Información.

La universidad con el deber de implementar un SGSI para salvaguardar sus activos de información, ha incurrido en errores considerados como aspectos fundamentales que deben ser contemplados desde la etapa de planeación dentro del ciclo de vida PHVA, a grandes rasgos deja evidencia la falta de compromiso y liderazgo del consejo superior universitario como alta dirección, ausencia de recursos, la inexistencia de una política de seguridad, ausencia de fechas establecidas, roles, responsables y un plan para valorar y tratar los riesgos entre otros. Por esta razón se menciona tanto la norma ISO 27001 como el framework COBIT 5, los cuales brindan un conjunto de actividades, procesos y buenas prácticas. Que mediante un procedimiento metódico ayuda a la universidad en la consecución de implementar un SGSI.

Índice de Términos—MinTIC, GEL, SGSI, ISO 27001, riesgos, seguridad de la información, COBIT 5, gobierno corporativo, gobierno de TI.

Abstract — The Ministry of Information Technologies and Communications MinTIC established a manual with which responsibilities are given in this case to the Francisco José de Caldas District University to implement among several activities an Information Security Management System.

The University with the duty to implement an ISMS to safeguard its information assets has incurred errors considered as fundamental aspects that must be contemplated from the planning stage within the PDCA Lifecycle, broadly demonstrating the lack of commitment and Leadership of the University Superior Council as Senior Management, absence of resources, lack of a Security Policy, absence of established dates, roles, responsible and a plan to assess and treat risks among others. This is why both the ISO 27001 standard and the COBIT 5 framework are mentioned, which provide a set of activities, processes and good practices. That through a methodical procedure helps the University in the achievement of implementing an ISMS.

Keywords— MinTIC, GEL, ISMS, ISO 27001, risks, information security, COBIT 5, Corporate Governance, IT Governance.

I. INTRODUCCIÓN.

El sistema de gestión de seguridad de la información definido como SGSI, describe un contexto global de procesos bien estructurados y

definidos que ayuden a mejorar y alcanzar los objetivos de misión y visión de cualquier organización. Por consiguiente, define un conjunto de normas y políticas que deben ser administradas con el propósito de asegurar la información y de esta manera lograr mantener la integridad, disponibilidad y confidencialidad de la misma. Producto de lo anteriormente enunciado, se expone en un entorno general la situación actual que vive la Universidad Distrital Francisco José de Caldas frente a temas de seguridad de la información y la implementación del SGSI.

Así mismo, se aborda el tema de la norma ISO 27001 la cual define los criterios que deben ser contemplados para establecer un SGSI, los cuales van encaminados al logro de los objetivos empresariales con una visión general de requisitos internos y externos sobre aspectos de seguridad de la información.

Finalmente se menciona COBIT 5 el cual brinda un entorno de negocio enfocado en el gobierno y la gestión de las tecnologías de la información para cualquier empresa. Con esto se busca alinear los objetivos de TI con los objetivos de negocio, con el propósito de satisfacer las necesidades de los interesados, abarcar en su totalidad la empresa, definir un único marco de referencia para lo cual separa las competencias y responsabilidades entre gobierno y gestión.

II. RESPONSABILIDAD DE LA UNIVERSIDAD FRENTE AL MINTIC.

Según lo establecido por el ministerio de las tecnologías de la información y las comunicaciones - MinTIC con el manual para la implementación de la estrategia gobierno en línea [1]. La Universidad Distrital Francisco José de Caldas como ente territorial del estado, está obligada a cumplir en el plazo pactado entre el año 2012 y 2017 con el nuevo modelo de gobierno en línea. Dicho manual describe cómo debe ser llevada a cabo la implementación del modelo, para lo cual define seis (6) componentes de carácter principal definidos según el decreto 2693 de 2012 [2] como:

	Información en línea	Interacción en línea	Transacción en línea	Transformación	Democracia en línea	Transversales
2013	40%	25%	15%	15%	40%	35%
2014	55%	50%	35%	35%	65%	60%
2016	80%	75%	70%	60%	95%	85%
2017	100%	100%	100%	100%	100%	100%

Fig. 1. Componentes y valores porcentuales de progreso en el tiempo que debe cumplir la Universidad Distrital FJC como ente Territorial [3].

El manual también menciona unas etapas de seguimiento y ejecución sobre el modelo de gobierno en línea para lo cual define:

Planeación y plazos: La universidad como entidad que debe ser parte del modelo de gobierno en línea - GEL, debe definir las actividades, responsables, metas y recursos necesarios para poder dar cumplimiento con lo definido en el decreto. Por lo tanto el MinTIC definió unos valores porcentuales a cada una de las actividades contenidas dentro de los seis (6) componentes, estableciendo plazos de implementación según su importancia y complejidad en el desarrollo.

Monitoreo y evaluación: La universidad se verá en la obligación de realizar su propio monitoreo y evaluación acerca del cumplimiento según lo establecido en el manual GEL para cada una de las actividades, en busca de lograr el escenario ideal sobre los niveles de madurez que define el manual hasta lograr el mejoramiento permanente.

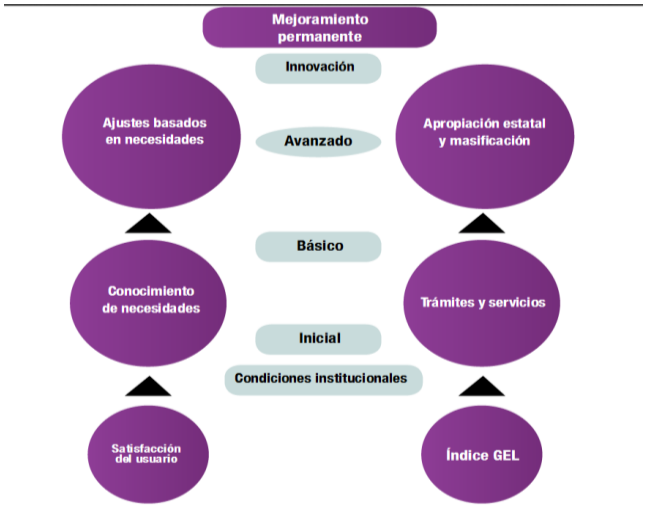

Fig. 2. Niveles de madurez de la Estrategia Gobierno en Línea [4].

Dentro de los seis (6) componentes definidos según el decreto 2693 de 2012 [5]. Enuncia que para alcanzar los objetivos definidos dentro del componente uno (1) denominado elementos transversales, se debe desarrollar 4 actividades entre las cuales se encuentra la de implementar un sistema de gestión de seguridad de la información (SGSI). Por esta razón, el manual de manera clara le indica a la universidad las actividades, herramientas y criterios que debe adoptar con el fin de lograr establecer un SGSI que contemple tanto los procesos misionales como los de apoyo.

Para tal fin, el manual propone que sea implementación un SGSI por medio de las fases definidas por el modelo de ciclo de vida "PHVA", asignando un porcentaje de 2.5%, 15%, 3.75% y 3.75% respectivamente sobre el avance en cada una de las fases.

De esta manera y para llevar a cabo en su totalidad el cumplimiento, es necesario contar con un SGSI para la universidad ya que es pieza integral dentro de los elementos transversales que hacen parte de los componentes enunciados en el manual para la implementación de la estrategia de gobierno en línea.

III. DEFINICIÓN DEL SGSI PARA LA UNIVERSIDAD DISTRITAL "FJC".

La universidad en hecho de cumplir por lo establecido por el MinTIC, establece una la resolución de la rectoría [6], en donde se creó el subsistema de gestión de seguridad de la información – SGSI el cual plantea el diseño, la implementación, el mantenimiento y la mejora continua de todos los procesos misionales y de apoyo en la institución con el propósito de lograr el aseguramiento de la confidencialidad, integridad y disponibilidad de los activos de información, logrando mitigar los riesgos a los que se ve enfrentada la universidad en cuanto a seguridad de la información.

Dentro de la creación se define el objetivo y el alcance que tiene el SGSI para la universidad, en el cual vincula absolutamente todos los procesos enmarcados dentro del modelo de operación por procesos definido por el sistema integrado de gestión de la universidad distrital - SIGUD.

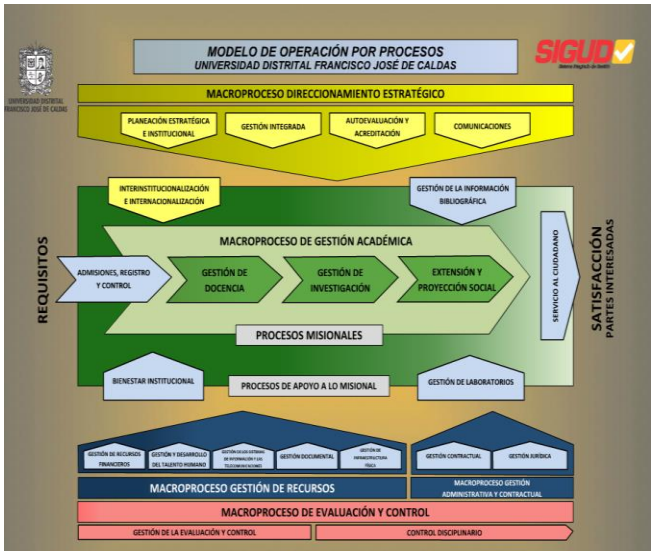

Fig. 3. Modelo de Operación por Proceso definido por la Universidad Distrital FJC [7].

Por consiguiente, para realizar un trabajo de aseguramiento de la información dentro del modelo de operación por procesos, se establecen tres actores que hacen parte integral para la implementación del SGSI en la universidad, a los cuales se les dictan las

responsables y las funciones que deben ser realizadas como miembros que hacen parte del comité, creados de la siguiente manera:

Coordinación del Subsistema: Será la dependencia secretaría general quien actuará con el compromiso de gestionar, planificar, coordinar y revisar las actividades y recurso del SGSI.

Comité de Gestión de la Seguridad de la Información: De este hacen parte la rectoría, la secretaría general, La oficina asesora de planeación y control, la oficina asesora de sistemas, la red de datos UDNET, la sección de actas archivo y microfilmación, la sección de biblioteca y la oficina asesora de control interno quien tiene voz pero no voto. Sobre ellos cae la responsabilidad de asesorar al consejo superior universitario – CSU quien es la figura de máximo órgano de dirección y gobierno de la universidad. Es responsabilidad de ellos también, lograr el aseguramiento de la información frente a la integridad, disponibilidad, confidencialidad, autenticidad y no repudio sobre los activos de información que posee la universidad logrando la mitigación, tercerización, aceptación o eliminación de los riesgos a los que está expuesta.

Grupos de Apoyo: Hacen parte servidores públicos y/o contratistas, los cuales aportarán conocimientos técnicos y especializados por medio de procesos y procedimientos que logren contribuir con el mejoramiento del SGSI de la universidad.

De esta manera la universidad busca inmiscuirse todos los factores necesarios que conlleven a lograr salvaguardar sus activos de información.

IV. LA PROBLEMÁTICA DE LA UNIVERSIDAD FRENTE SGSI.

La universidad, en el caso de implementar la estrategia gobierno en línea – GEL establecido por el ministerio de las tecnologías de la información y las comunicaciones – MinTIC y en particular sobre la definición del SGSI ha incurrido en errores los cuales hacen que falle frente al compromiso ante el MinTIC.

La universidad hasta la fecha no ha definido presupuesto de inversión o de funcionamiento mediante un rubro, con el cual se pueda llevar a cabo el desarrollo del SGSI. Indiscutiblemente la universidad es una entidad que debería dentro de su organigrama definir el área o dependencia de seguridad de la información e informática y por consiguiente mediante trabajo mancomunado con otras dependencias lograr la implementación del SGSI.

La universidad al momento de definir el alcance del SGSI contempló todos los procesos misionales y de apoyo que realiza, lo cual no es un problema el querer implementar el SGSI en la institución. El problema realmente radica es que a momento la universidad no cuenta con un inventario de activos de información, tampoco dispone de una guía para la identificación de activos de información, no cuenta de un formato para el levantamiento de activos de información y una tabla para la valoración de activos en el cual se contemplen los niveles de criticidad y probabilidad de impacto, y sumado a todo esto también se carece de los responsables de llevar a cabo estas funciones.

La universidad por medio de varias de sus dependencias dispone de diversos sistemas o aplicaciones, con lo cual se dificulta tener centralizada la información al momento de disponer de ella. Otros sistemas fueron desarrollados a la medida, pero presentan problemas sobre la integridad de la información que reposa en sus bases de datos, evidenciando duplicidad, falta de control de históricos e información incompleta y a esto sumando la carencia de un gestor documental de modo que se pueda administrar la documentación durante todo su proceso de ciclo de vida.

La universidad dentro del SGSI no tiene definido de manera clara un equipo de respuesta a incidentes de seguridad de la información – CERT ó CSIRT. El cual se encargue de prevenir, mantener y mitigar incidentes de seguridad frente a los que puedan estar expuestos los activos de la institución.

El desconocimiento de una política de seguridad de la información o la no existencia de la misma en la universidad. Repercute directamente sobre la identificación de compromisos y responsables capaces de cumplir los objetivos de seguridad de la información definidos en el SGSI.

Falta trabajo en conjunto entre las dependencias de recursos humanos y la oficina asesora jurídica, para que desde los procesos contractuales se realice una selección idónea de personal y dentro de las cláusulas sean definidas las responsabilidades frente al conocimiento y ejecución de procedimientos de seguridad de la información dentro de la institución.

En la universidad existe la cultura o pensamiento de que los temas relacionados con seguridad de la información son de la competencia de las áreas de TI, así como la implementación y el mantenimiento del SGSI. Por tal motivo la responsabilidad recae sobre las dependencias oficina asesora de sistemas y la red de datos UDNET. En consecuencia, muchos procesos llevados a cabo en la universidad que no están soportados por estas dependencias están aún más expuesto frente riesgos de seguridad de la información.

En la universidad no se ha llevado a cabo un plan concientización a los trabajadores sobre temas de seguridad de la información, de tal manera que se busque proteger o prevenir el activo humano frente posibles riesgos de seguridad de la información.

La universidad no ha hecho un proceso de evaluación inicial para conocer así mismo como se encuentra frente a temas relacionados con seguridad de la información. En consecuencia, el desconocimiento puede repercutir directamente en la asignación de recursos y ejecución de procesos para la implementación del SGSI.

En el comité definido por la universidad existe desconocimiento sobre seguridad de la información de forma parcial y en algunos casos de forma total, en personas o dependencias que hacen parte del comité definido para la implementación del SGSI. Lo cual repercute directamente en el desarrollo y toma de decisiones sobre lo que se establece que debe tener el SGSI.

La universidad además de la resolución en donde se crea el SGSI, no cuenta con la documentación necesaria que hacen parte del SGSI. En algunos casos como las áreas de TI, se tiene documentación que ayuda a proteger los activos de información pero estos no se encuentran debidamente oficializados y comunicados al personal de la universidad.

La universidad no cuenta con una planificación y gestión del SGSI. De tal modo que las actividades y procesos a realizar no tienen responsables ni fechas de ejecución afectando la coordinación y completa implementación del SGSI

V. ISO27001 COMO MARCO DE REFERENCIA.

La norma ISO 27001:2013 [8] se define como un estándar que contempla generalidades enmarcadas dentro de una metodología sugerida con el fin de suministrar los requisitos necesarios para implementar un sistema de gestión de seguridad de la información. Dicha norma hace parte de la familia ISO 27000 que indiscutiblemente suministra un marco global de gestión de seguridad de la información para ser implementado en entidades tales como lo son las del estado, industriales, financieras, de seguros y hasta las del sector salud.

La norma de manera inmersa define un modelo de ciclo de vida PHVA o PDCA (siglas en inglés) que en particular busca la manera de definir, implementar y que se lleve un adecuado mantenimiento en busca de lograr una mejora continua del SGSI. Por esta razón se considera que el SGSI debe ir de la mano con los objetivos y necesidades definidos por la organización como resultado del logro de la preservación de la confidencialidad, disponibilidad e integridad de los activos de información a través de un proceso adecuado de gestión sobre los riesgos de seguridad de la información a los que se ve expuesta la entidad.

La norma como estándar internacional para la certificación exige a toda organización sin exclusión alguna que adopte del numeral 4 al numeral 10. En consecuencia, los procesos y actividades definidos en estos numerales se pueden integrar de manera global dentro del ya antes mencionado ciclo de vida PHVA.

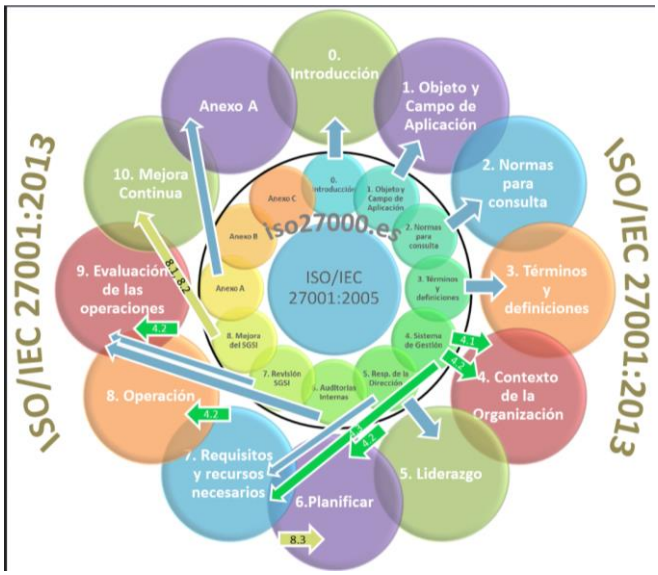

Fig. 4. Diagrama de cláusulas principales de la versión 2005 y la versión 2013[9].

Por consiguiente, adoptando el ciclo de vida PHVA se logra representa los lineamientos de las actividades y procesos que menciona en cada numeral la norma, los cuales se deben implementar de conformidad para lograr la certificación ISO 27001:2013.

VI. COBIT 5 COMO MARCO DE REFERENCIA.

COBIT 5 es un framework o marco de negocio para el gobierno y la gestión de las tecnologías de la información de la empresa [10] desarrollado por ISACA (*Information System Audit and Control Association)*.

COBIT 5 es una estructura de trabajo unificada que aporta el logro o consecución de los objetivos empresariales por medio del gobierno y gestión de las tecnologías de la información, por consiguiente el framework realiza la adopción de cinco principios fundamentales.

Fig. 5. Principios de COBIT 5 [11].

Dentro del marco general de COBIT 5 se atribuye al gobierno corporativo, el establecer, mantener, dar compromiso, roles y responsabilidades sobre los recursos y procesos que apoyen el programa. Para ello es necesario se logre el aseguramiento de la dirección estratégica para el alcance de los objetivos de forma tal que se consiga gestionar los riesgos de manera idónea y de esta forma lograr obtener el equilibrio entre la conformidad y el desempeño empresarial.

Al hablar de gobierno corporativo subyace la figura de gobierno de TI. Quien se encarga de entregar valor por medio de lograr alinear los procesos y operaciones con los objetivos de la empresa, debe estar en la capacidad de administración y gestión de los riesgos, hacer uso eficiente y adecuado de los recursos, salvaguardar los activos de información, medir el desempeño de procesos aplicados y servicio entregado.

El modelo de referencia de COBIT 5 establece un conjunto completo de 37 procesos dividiéndolos en 5 que enmarcan lo de gobierno y 32 asociados a cuatro dominios que comprende la gestión.

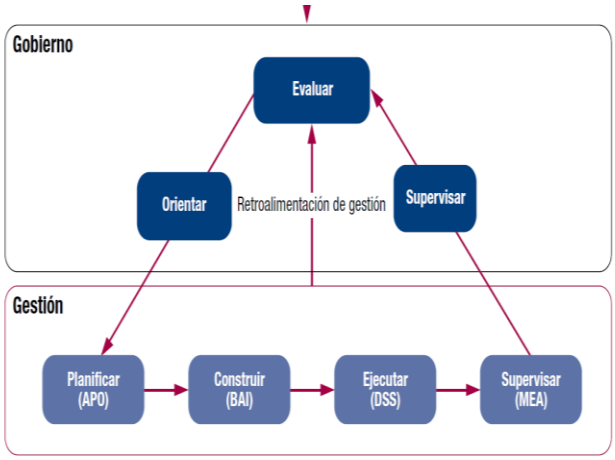

Fig. 6. Áreas clave de gobierno y gestión COBIT 5 [12].

COBIT 5 en cuanto a que no permite certificación, presenta un modelo completo de procesos sobre tecnologías de la Información con los cuales se busca estar enfocado en el negocio u objetivos empresariales, basándose en la implementación de controles y en la medición del desempeño de implementación.

VII. CONCLUSIONES.

En el presente, las tecnologías de la información evolucionan de manera vertiginosa, lo cual hace que la demanda de información sea cada vez mayor. De esta manera, se debe trabajar en la gestión y administración del riesgo frente a la que está expuesta la información, y por consiguiente garantizar la integridad, confidencialidad y disponibilidad de la misma.

La seguridad de la información debe verse como una actividad continua, dado que los activos de información de una compañía nunca estarán completamente protegidos frente a riesgos e incidentes de seguridad.

La seguridad de la información debe verse como una actividad continua, dado que los activos de información de una compañía nunca estarán completamente protegidos frente a riesgos e incidentes de seguridad.

La universidad no ha tomado conciencia del valor y responsabilidad que tiene de proteger sus activos frente a los riesgos que está expuesta, evidencia de eso es el poco progreso alcanzado al definir e implementar un sistema de gestión de seguridad de la información. Además de ello, la universidad difícilmente pueda cumplir con lo estipulado por el MinTIC sobre las fechas para implementar la estrategia de gobierno en línea. En consecuencia puede incurrir en faltas, detrimento y hallazgos por los entes que la controlan.

Debe existir un compromiso pleno por parte del consejo superior universitario que garantice los recursos necesarios de implementación y mejora continua del SGSI, establecer una correcta planeación, incluyendo fechas definidas y responsables sobre las actividades y procesos a lo largo de la ejecución del SGSI.

Para lograr implementar el SGSI en la universidad debe existir una participación en conjunto entre personas y/o dependencias con conocimiento y aptitudes para ser parte del proceso, lo cual simplifique o acorte los esfuerzos en la ejecución de las actividades.

La universidad debe establecer una política de seguridad de la información, que esté documentada, comunicada y sea de obligatorio cumplimiento para toda la institución sin excepción alguna.

El conocimiento y apropiación de la norma ISO 27001 le brinda a la universidad una metodología completa junto con los objetivos de control y controles que puede contemplar para la correcta implementación de un SGSI.

COBIT 5 como marco de referencia ofrece lineamientos con los objetivos de la universidad por medio de los procesos enmarcados en el gobierno y gestión de tecnologías de la información. Desarrollando políticas claras, cierre de brechas, gestión de riesgos de negocio y buenas prácticas.

REFERENCIAS.

[1] Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la República de Colombia. Disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

[2] Decreto número 2693 de 2012 del Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en: http://www.mintic.gov.co/portal/604/articles-3586_documento.pdf

[3] Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la República de Colombia. Disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

[4] Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la República de Colombia. Disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

[5] Decreto número 2693 de 2012 del Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en: http://www.mintic.gov.co/portal/604/articles-3586_documento.pdf

[6] Resolución de la Rectoría número 632 del 03 de Diciembre de 2015 de la Universidad Distrital Francisco José de Caldas. Disponible en: http://sgral.udistrital.edu.co/xdata/rec/res_2015-632.pdf

[7] Modelo de Operaciones por Procesos de la Universidad Distrital FJC. Disponible en: http://comunidad.udistrital.edu.co/sigud/procesos/

[8] (2013, Diciembre). NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001.

[9] Diagrama Cláusulas comparación ISO 27001:2005 e ISO 27001:2013. Disponible en: http://www.iso27000.es/iso27000.html#seccion1

[10] ISACA. (2012). COBIT 5 AN ISACA FRAMEWORK. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.

[11] ISACA. (2012). COBIT 5 AN ISACA FRAMEWORK. Principios de COBIT 5, pp 13.

[12] ISACA. (2012). COBIT 5 AN ISACA FRAMEWORK. Las Áreas clave de Gobierno y gestión COBIT 5, pp 32.

Rojas Villamil, Carlos Michael.